DFARS Case 2012-D055
Final Rule 79 Fed. Reg. 26092 (Effective May 6, 2014)
Public Meeting: Detection & Avoidance of Counterfeit Electronic Parts – Further Implementation

The new DFARS Rule: Compliance and Business Risks

Robert S. Metzger
Rogers Joseph O'Donnell, P.C.
750 Ninth Street, N.W., Ste 710
Washington, D.C. 20001
(202) 777-8951
rmetzger@rjo.com www.rjo.com

Rogers Joseph O'Donnell © 2014 All Rights Reserved

Counterfeit Parts Regulations Risk Assessment

Subject Clause or Requirement	Compliance Risk	Business Risk	Industry Readiness
Legacy Inventory / DFARS Applicability (Preamble)	**HIGH** • Inventory not procured in connection with a previous DoD contract is subject to traceability and authentication requirements.	**HIGH** • Implies legacy inventory bought from brokers needs to be reevaluated in accordance with current standards and methods. • Authority of contractors to employ inventory is uncertain even with additional measures to assess and mitigate risk.	**RED**
DCMA CPSR Surveillance **252.246-7007(d)** **246.870-2** **252.244-7001**	**MED** • Unknown if DCMA would consider an escape a deficiency.	**MED** • All existing contracts with DFARS 252.242-7005 Contractor Business Systems invoked. • It is unknown what DCMA would consider a deficiency significant enough to invoke penalties.	**YELLOW**
Contract Flow Down **246-870-2(b)(9)** **252.246-7007(c)(9)** **252.246-7007(e)**	**MED** • Contractual flow down with wide interpretation of the complex regulation.	**MED** • Stalled contract negotiations on clauses/risk business is unwilling to accept. • Increased liability introduced from complex clauses received from customers not understood by Contract Managers. • Suppliers unwilling to accept flow down. • Continuity of supply, esp. from small business.	**YELLOW**
Allowable Costs for Counterfeit & Suspect Counterfeit **231.205-71**	**LOW** • Impact limited to Prime CAS-Covered contracts and flow down. • Risk becomes greater for lower-tier downstream suppliers if clause is accepted.	**HIGH** • The cost of counterfeit electronic parts and suspect counterfeit electronic parts and the cost for rework or corrective action that may be required are not allowable under Department contracts. • Not clear how to separate allowable costs of investigation from unallowable costs once a part is deemed “suspect”.	**YELLOW**
Control of Obsolescence **246-870-2(b)(12)** **252.246-7007(c)(12)**	**MED** • Unclear if expectation is for contractors to control issue for unfunded DMSMS programs. • Lower tier suppliers unlikely to have DMSMS programs.	**MED** • Cost to remediate obsolescence or fund Last-Time-Buys may still be an unfunded mandate. • Impact to commercial programs due to common items and dual-use. • Lower tier contractors will likely increase costs to implement a program due to flow down requirement.	**YELLOW**

Counterfeit Parts Regulations Risk Assessment

Subject / Source of Requirement	Compliance Risk	Business Risk	Industry Readiness
Reporting & Quarantining **246-870-2(b)(6)&(b)(11)** **252.246-7007(c)(6)&(c)(11)** **Additional FAR Case Pending for Reporting**	**MED/HIGH** • It will be difficult to segregate items destined for DoD due to dual-use and common items. • **New Proposed FAR rule also requires reporting of nonconforming "common items" and is applicable to all government agencies.**	**MED/HIGH** • Payment issues due to quarantining. • Potential of DCMA targeting due to reports.	**RED**
Traceability **252.246-7007(c)(11)**	**HIGH** • Supply chain unable to support traceability requirement as written "clear identification of the name and location Of supply chain intermediaries from the manufacturer to the direct source of the product for the seller" • Guidance not available on what to do (e.g. waiver) for each item without traceability. • **Pending DFARS Case 2014-D005 is expected to address qualification of "additional" trusted suppliers – e.g, "broker" parts**	**HIGH** • Non-pedigree EEE inventory from brokers will be unable to comply.	**RED**
Definition of "Electronic Part"	**HIGH** • Term introduces embedded firmware and software which now implies cyber physical security concerns • Access to threat information problematic at present • Detection outside ordinary QA capability • Includes circuit assemblies • Additional complications due to COTS Assemblies (e.g. CISCO Router)	**HIGH** • Currently no industry or government standard to comply. • There are industry acknowledged gaps in vulnerability on this topic.	**RED**
COTS **Applicability (Preamble)**	**MED** • Unclear what to do (waiver or deviation?) for each item/supplier unwilling to accept requirements. • Implies requirements down to piece part assembly for COTS suppliers. • Ability of commercial sources to accommodate system requirements very dubious	**MED** • Industry may not have enough influence with COTS suppliers to invoke requirements. • Continuity of supply	**RED**
Use of suppliers that are the original mfg. **246-870-2(b)(5)**	**MED** • Unclear if use of brokered parts for long lead production or obsolete items is prohibited without some affirmative gov't action (CO approval or waiver?) due to conflict with 246-870-2(b)(5) CPSR system criteria	**MED/HIGH** • Production stoppage if requirement mandates prohibiting	**YELLOW**

Red text indicates expected requirements through further implementation in pending regulations

Speaker: Robert S. Metzger

Robert S. Metzger received his B.A. from Middlebury College and is a graduate of Georgetown University Law Center, where he was an Editor of the *Georgetown Law Journal*. He was a Research Fellow, Center for Science & International Affairs, Harvard Kennedy School of Government.

Mr. Metzger is the Managing Partner of the Washington, D.C. office of Rogers Joseph O'Donnell, P.C. He is a member of the International Institute for Strategic Studies (IISS), London. Academic publications on security topics include articles in *International Security*, the *Journal of Strategic Studies* and *Indian Defence Review*. He is a Vice-Chair of the Supply Chain Assurance Committee of TechAmerica. He is recognized as a leading national expert on supply chain assurance and cyber risk management. He is ranked in 2014 *Chambers USA* as a top Government Contracts lawyer (national).

Rogers Joseph O'Donnell is a boutique law firm that has specialized in public contract matters for 33 years. It is ranked in "Band 2" by the 2014 *Chambers USA* – the only boutique among the nine highest ranked firms.
Mr. Metzger advises leading US and international companies on key public contract compliance challenges and in strategic business pursuits.

SELECTED EXTERNAL PUBLICATIONS
available at http://www.rjo.com/metzger.html

- "Convergence of Counterfeit and Cyber Threats: Understanding New Rules on Supply Chain Risk," *Federal Contracts Report*, Feb. 18, 2014
- "DoD Counterfeit Parts Rule – So Little After So Long," *Law360* , Jun. 5, 2013
- "New DOD Counterfeit Prevention Policy: Resolves Responsibilities Within DOD But Leaves Many Contractor Questions Unresolved," (PDF) *Federal Contracts Report*, May 15, 2013
- "Counterfeit Electronic Parts: What to Do Before The Regulations (and Regulators) Come? (Part 2)," *Federal Contracts Report*, Aug. 21, 2012
- "Counterfeit Electronic Parts: What to Do Before the Regulations (And Regulators) Come? (Part 1)," *Federal Contracts Report*,4 - Jun. 21, 2012 (with Jeff Chiow)